ORDERING GUIDE

FortiAnalyzer

Product Offerings

Available in:

Appliance | Virtual Machine | Cloud

FortiAnalyzer provides central logging and reporting, advanced analytics, and security automation for rapid detection and response against cyber threats.

The product offering includes:

- **FortiAnalyzer Appliance**: on-premise solution provides the best response times and detection technology with the full range of features and benefits.
- **FortiAnalyzer Perpetual VM**: virtual appliance offering supported across public and private clouds.
- **FortiAnalyzer VM Subscription**: subscription based offering of the VM model, that bundles support and services.
- **FortiAnalyzer Cloud**: subscription to cloud-based central logging & analytics.

This ordering guide provides a consolidated reference to the relevant FortiAnalyzer products and services available to your organization

	150G	300G	800G	1000F	3000G	3500G	3700G	4500F	FAZ-VM	BD-VM	CLOUD
GB/Day	**25**	**100**	**200**	**660**	**3,000**	**5,000**	**8,300**	**20TB**	**Stackable**	**Stackable**	**Stackable**
Sustained LPS	500	2,000	4,000	20,000	42,000	60,000	100,000	300,000		Stackable	
Collector Mode Sustained LPS	750	3,000	6,000	30,000	60,000	90,000	150,000				
No. Days @ Max Sustained LPS	90	50	50	34	30	38	60	30		Stackable	
Max Devices/VDOMs	50	180	800	2,000	4,000	10,000	10,000	10,000+	10,000	10,000	10,000
Max ADOMs	35	25	50	50	500	500	1,200	2,500	1,200	1,200	
Max ADOMs with add-on license					1,200		10,000				
Distributed Arch. / Horizontal Scaling								✓		✓	
Container Modules Supported											
FortiSOAR				7.0	7.0	7.0	7.0		7.0		
Security Services											
FortiGuard IOC Service	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security Automation Service	✓	✓	✓	✓	✓	✓	✓	7.0	✓	✓	✓
FortiGuard Outbreak Detection Service	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0
FortiCASB ShadowIT	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0	7.0
SIEM Database Capable	✓	✓	✓	✓	✓	✓	✓	7.0	✓	7.0	✓
UEBA Database Capable	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Additional Services											
FortiCare Premium Contract				Subscription							
FortiCare Elite Contract						Subscription					
Replacement Disks				✓	✓	✓	✓	✓			
How to Buy	**Hardware Bundle**	**Hardware Bundle**	**Hardware Bundle**	**Hardware Bundle**	**Hardware Bundle**	**Hardware Bundle**	**Hardware Bundle**	**Hardware Bundle**	**VM Bundle/ Subscription**	**VM Bundle**	**FortiGate Subscription**

ORDER INFORMATION

FORTIANALYZER	HARDWARE DEVICES							
	150G	300G	800G	1000F	3000G	3500G	3700G	4500F (FAZ-BD)
Hardware	FAZ-150G	FAZ-300G	FAZ- 800G	FAZ- 1000F	FAZ- 3000G	FAZ- 3500G	FAZ- 3700G	FAZ-BD-4500F
Hardware Bundle	FAZ-150G-BDL-466-DD	FAZ-300G-BDL-466-DD	FAZ-800G-BDL-466-DD	FAZ-1000F-BDL-466-DD	FAZ-3000G-BDL-466-DD	FAZ-3500G-BDL-466-DD	FAZ-3700G-BDL-466-DD	FAZ-BD-4500F-BDL-466-DD
Renew Bundle	FC-10-L150G-466-02-DD	FC-10-L03HG-466-02-DD	FC-10-L08HG-466-02-DD	FC-10-L01KF-466-02-DD	FC-10-L03KG-466-02-DD	FC-10-L3K5G-466-02-DD	FC-10-L3K7G-466-02-DD	FC-10-BD45F-466-02-DD
Support-only Renewal	FC-10-L150G-247-02-DD	FC-10-L03HG-247-02-DD	FC-10-L08HG-247-02-DD	FC-10-L01KF-247-02-DD	FC-10-L03KG-247-02-DD	FC-10-L3K5G-247-02-DD	FC-10-L3K7G-247-02-DD	FC-10-BD45F-247-02-DD
Replacement Disks								
Replacement Disk SKU				SP-FMG1KF-HDD	SP-D4TC	SP-FAZ-3500G-SATA-HDD	SP-DAM37G4T	SP-BD4500F-SSD-B1 SP-BD4500F-SSD-B2
Replacement PSUs								
Replacement PSU SKU		SP-FAD400F-PS	SP-FAZ800G-PS	SP-FMG400E-PS	SP-FAZ3000G-PS		SP-FAZ3700F-PS	SP-BD4500F-PS (module only)

FORTIANALYZER VM							
	5GB/Day		50GB/Day		500GB/Day		Description
Subscription Bundles	FC1-10-AZVMS-465-01-DD		FC2-10-AZVMS-465-01-DD		FC3-10-AZVMS-465-01-DD		All in one subscription bundle including 24×7 FortiCare Premium Support, IOC, Security Automation Service, and FortiGuard Outbreak Detection service. Fully stackable.
	1GB/Day	5GB/Day	25GB/Day	100GB/Day	500GB/Day	2000GB/Day	
Perpetual License	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000	Perpetual license. Purchase 24×7 FortiCare Premium Support, IOC, Security Automation Service, and FortiGuard Outbreak Detection Service separately. Only GB/Day is stackable.

FORTIANALYZER BD-VM				
License Type	**SKU**	**Logs/Sec**	**Storage capacity**	**Description**
Base License	FAZ-BD-VM	150,000	200 TB	FortiAnalyzer-BD virtual appliance with 150,000 logs/sec ingestion rate and 200TB storage capacity to start. Support add-on to scale up performance and storage.
Add-On License	FAZ-BD-VM-UG	50,000	50 TB	FortiAnalyzer-BD virtual appliance ADD-ON to add additional capacity with 50,000 logs/sec ingestion rate and 50TB storage. Multiple ADD-ONs can be stacked together to scale up the ingestion rate and storage.

FORTIANALYZER CLOUD				
				Description
Per Device Subscription	FC-10-[FortiGate Model Code]-464-02-DD			FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service, and SOCaaS.
Per Device Subscription	FC-10-[FortiGate Model Code]-585-02-DD			FortiAnalyzer Cloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, and FortiGuard Outbreak Detection Service.
	5GB/Day	**50GB/Day**	**500GB/Day**	
Cloud Storage Add-On	FC1-10-AZCLD-463-01-DD	FC2-10-AZCLD-463-01-DD	FC3-10-AZCLD-463-01-DD	FortiAnalyzer Cloud Storage Add-on for FortiGate logs and all other supported Fortinet product logs. Including FortiCloud SOCaaS. Stackable

EXTENSIONS		
EXTENSION	**EXTENSION LICENSE**	**Description**
FortiSIEM Collector	Included in FortiAnalyzer	Collect and forward FortiAnalyzer events to FortiSIEM
FortiSOAR	FC-10-SRVMS-389-02-DD	FortiSOAR Enterprise Subscription plus 24×7 FortiCare and FortiCare Best Practice Service - 2 User Logins included

FORTIANALYZER VM: PRIVATE CLOUD SUPPORT							
	VMware	**Citrix Xen**	**KVM**	**Microsoft Hyper-V**	**Nutanix AHV**	**Oracle Private Cloud**	**OpenSource Xen**
FAZ-VM	✓	✓	✓	✓	✓	✓	✓

FORTIANALYZER VM: PUBLIC CLOUD SUPPORT				
	Amazon AWS	**Microsoft Azure**	**Google GCP**	**Oracle OCI / OPC**
FAZ-VM	✓	✓	✓	✓

NSE TRAINING AND CERTIFICATION

Fortinet NSE 5: FortiAnalyzer
Instructor-led learning the fundamentals of using FortiAnalyzer for centralized logging and reporting:
- **FT-FAZ** - NSE 5/FAZ Training - 2 days

Certification Exams
NSE 5 Network Security Analyst:
- **NSE-EX-SPL5**

Pre-requisites
- Familiarity with all topics presented in the NSE 4 FortiGate Security and NSE 4 FortiGate Infrastructure courses
- Knowledge of SQL SELECT syntax is helpful, but not required

References
Course description
https://training.fortinet.com/local/staticpage/view.php?page=library_fortianalyzer

FREQUENTLY ASKED QUESTIONS

What is the FortiGuard Outbreak Detection Service and how do I purchase?
What is FortiGuard Outbreak Detection Service?
- The FortiGuard Outbreak Detection Service, provides customers with content packages created in real time, to protect their networks against new malware outbreaks. The package contains reports, report templates and event handlers to handle the latest malware outbreaks identified by Fortinet's Global Threat Intelligence.

How do I purchase FortiGuard Outbreak Detection Service?
- The FortiGuard Outbreak Detection Service is included with the FortiAnalyzer Enterprise Protection bundle and is available a la carte for eligible hardware models.
- The FortiGuard Outbreak Detection Service is available a la carte for FortiAnalyzer Perpetual VM.
- The FortiGuard Outbreak Detection Service is included with FortiAnalyzer VM Subscription.

What is SOCaaS, what is included with SOCaaS (SOC as as Service) and how do I purchase?
What is SOCaaS?
- SOCaaS is a Cloud-based managed security service offering – whereas Fortinet SOC analysts monitor the customer's network for security events and threats and escalate back to customer when detected.

What does SOCaaS include?
- 7×24×365 monitoring of security events and device health for FortiGate firewalls
- Incident detection, investigation and escalation
- Preventative control review and tuning recommendation
- Weekly/Monthly reports & quarterly risk review
- Remote assistance via online chat, email, and phone
- Access to the SOCaaS Portal

How do I purchase SOCaaS?
- FortiAnalyzer Cloud with SOCaaS can be purchased for supported FortiGate models. Each FortiGate requiring the monitoring service requires a license.

How do I purchase a VM perpetual license?
A VM perpetual license can be purchased in two ways.
1. Start with a limited free trial (available with a FortiCloud account) then upgrade the VM by purchasing an upgrade license SKU to increase capacity.
2. Purchase an upgrade license SKU directly.

How do I extend my existing FAZ VM Perpetual deployment?
Customers who already have a perpetual FAZ-VM can purchase any of the below add-on SKUs to extend the capacity of their existing FAZ-VM deployment.

SKU	DESCRIPTION
FAZ-VM-GB1	Upgrade license for adding 1 GB/Day of Logs.
FAZ-VM-GB5	Upgrade license for adding 5 GB/Day of Logs.
FAZ-VM-GB25	Upgrade license for adding 25 GB/Day of Logs.
FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs.
FAZ-VM-GB500	Upgrade license for adding 500 GB/Day of Logs.
FAZ-VM-GB2000	Upgrade license for adding 2 TB/Day of Logs.

What is included in FAZ-VM Free Trial and how many trials can I have?
The FortiAnalyzer VM Free Trial includes the following:
- 1 GB/day logs, 3 devices, 3 ADOMs.
- Trial licenses do NOT include services or support.

How many free trials can I have?
- Customer can generate 1 free trail for a product on their account at a time.
- Only 1 free trial per product, per account, can be active at a time.
- Once the purchased add-on license is applied to the trial instance, the trial instance is converted into Production Instance.
- Only after the free trial is converted to the production instance, will a new free trial be available again for the FortiCare account.
- Once a product has no active free trial on the FortiCare account, a new free trial will be available.

*So, a customer can generate multiple Trial Licenses but not at the same time.
**For PoCs or for our Demo Labs we still have the Eval Licenses. 60-days for external or 1 Year for internal.

Can I opt-out of the FortiCare Free Trial and directly purchase a license?
Customers can opt out of the free trial and purchase only the FortiAnalyzer-VM stackable add-on SKUs.
- For FortiAnalyzer 7.0 customers will receive a license and can enter the purchased license code on the VM login page. Customers can also upload new licenses via the GUI.
- For FortiAnalyzer 6.2/6.4 customers, licenses can be uploaded via the GUI.

How many ADOMs are included with my FortiAnalyzer?
ADOM defaults and maximums information for FortiAnalyzer Hardware and VM can be found on docs.fortinet.com in the release notes for your FortiAnalyzer's firmware release under Appendix A.

How do I add ADOMs to my FortiAnalyzer?
- An ADOM add-on license can be purchased for FortiAnalyzer VM Subscriptions, and for supported FortiAnalyzer hardware models (FortiAnalyzer hardware G models 1000 Series and above)
- The ADOM add-on License SKUs for FortiAnalyzer can be found under the "VDOM & ADOM" tab of the pricelist.

How do I order FortiAnalyzer cloud?
FortiAnalyzer Cloud and FortiAnalyzer SOCaaS for FortiGates are obtained via the below SKUs

SKU	DESCRIPTION
FC-10-[FortiGate Model Code]-464-02-DD	FortiAnalyzer Cloud with SOCaaS: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service and SOCaaS.
FC-10-[FortiGate Model Code]-585-02-DD	FortiAnalyzer Cloud: cloud-based central logging and analytics. Include all FortiGate log types, IOC service, Security Automation Service, FortiGuard Outbreak Detection Service.

How do I order more storage for my FortiAnalyzer cloud?
- FortiAnalyzer Cloud Storage can be increased by purchasing the stackable "FortiAnalyzer Cloud Storage" SKU in the Cloud tab of the pricelist.

www.fortinet.com

FAZ-OG-R12-20230213